# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicant: | Perlmutter, et al. | Examiner: | D. Duong |
| Serial No.: | 09/740,052 | Art Unit: | 2663 |
| Filed: | 12/19/2000 | Attorney Docket No.: | NN-13361 |
| Title: | BANDWIDTH MANAGEMENT FOR TUNNELING SERVERS | | |

CERTIFICATE OF MAILING

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being deposited with the United States Postal Service as first class mail under 37 C.F.R. 1.8, and is addressed to M.S. Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 10, 2004.

John C. Gorecki

John C. Gorecki, Reg. No. 38,471

M.S. Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450



## APPELLANT'S BRIEF

(1) Real Party In Interest

This application is owned by Nortel Networks, Limited, of St. Laurent, Quebec, CANADA.

(2) Related Appeals and Interferences

None

(3) Status of Claims

Claims 2 and 11 have been canceled.

Claims 1, 3-10, and 12-18 are pending in the application and stand rejected.

(4) Status of Amendments

There are no un-entered amendments.

(5) Summary of invention

This invention relates to a method for a server to manage bandwidth of a link not directly connected to the server, to enable differentiate classes of service of traffic to use the link without requiring modification of routers forming a path through the network. (Specification at p. 2, lines 6-7). By allowing bandwidth to be metered on a per-application group basis, different application groups can share a link fairly by causing packets within an application group to contend for bandwidth allocated to that application group, and to not contend for bandwidth allocated to other application groups. (Specification at p. 4, line 21 to p. 5, line 4).

(6) Issues

Whether claims 1, 3-10, and 12-18 are unpatentable under 35 USC 103 over Ma et al (Ma) (U.S. Patent No. 5,953,338) in view of Arrow et al (Arrow) (U.S. Patent No. 6,175,917).

(7) Grouping of claims

The claims stand or fall together.

(8) Argument

The combination of Ma and Arrow fails to teach or suggest a VPN server that meters packets and authenticates, encapsulates, or de-encapsulates the packets that are being metered.

The Examiner has taken the position that Ma discloses a system for managing bandwidth of a remote link in a VPN 170 (Fig. 1) comprising a server 160 (Fig. 2, Col. 7 lines 5-14), a contention pool 401 or 402 having a portion of the bandwidth for at least one application group (Fig. 4A Col. 11 lines 11-26) and a meter 145 for metering the packets belonging to the application group. The Examiner admits that Ma fails to teach that the server is a VPN server configured to authenticate, encapsulate or de-encapsulate at least a portion of the packets, but

contends that Arrow teaches a server that performs these functions. Thus, the Examiner concludes that it would have been obvious to combine Arrow with Ma to provide this added functionality to the server in Ma. Applicants respectfully submit that this is incorrect, because neither Ma nor Arrow teach a server that assigns bandwidth of a link, meters packets on the link, and authenticates, encapsulates, or de-encapsulates the packets that are being metered.

The server in Ma is a central server, and not a VPN server as admitted by the Examiner. More specifically, the server 160 in Ma is a "centralized control module" that interfaces with ATM edge switches 130A, 130B, ... 130F to control each individual ATM edge switch. In so doing, the centralized control module 160 "controls the creation and nature of virtual paths and virtual channels extending throughout the overall ATM Network 120 (in FIG. 1B). (Ma at Col. 6, lines 57-63).

The central control server 160 includes a bandwidth manager module 150, a centralized call admission control usage monitor, and a call control module 140. As shown in Fig. 2 of Ma, these modules work together to dynamically adjust the amount of bandwidth to be provided to a VPN, and interface with the ATM switches to cause the ATM switches to adjust the size of the virtual path. This function is further discussed at Col. 8, lines 41-67 of Ma. Specifically, in this section, Ma states that the centralized control module 160 allows a carrier to make unused capacity on the network to clients by changing the size of the virtual paths on the network, and interfaces with the ATM switches over their respective management interfaces to cause the ATM switches to implement the newly sized VPN paths on the network.

Thus, the central control server 160 in Ma is a centralized device that is not configured to handle packets on the network. This central server does not encapsulate, de-encapsulate, or

authenticate packets that are being metered. Instead, the central server operates in a management capacity on the network, and does not handle packets on the links that it is managing.

Claim 1 recites a method for a VPN server that manages bandwidth of a remote link by assigning a portion of the bandwidth of the remote link to at least one application group, and metering packets belonging to the application group. Claim 1 further recites that the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets. The term "the packets" clearly refers back to the packets that are metered by the VPN server. Thus, claim 1 recites a method for a VPN server that meters packets and also performs at least one of authenticating, encapsulating, and de-encapsulating the packets.

A centralized control module cannot meter packets on the links and perform one of the claimed operations on the packets on the links, since the centralized control does not have access to the packets. Rather, Ma teaches that the central control operates in a management capacity and interfaces ATM switches via a conventional management interface, and that the ATM switches then handle the packets in a conventional manner.

The Examiner admits that Ma fails to teach that the server (centralized control module 160) is a virtual private network VPN server configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets. (Final Office Action at page 2,). However, the Examiner has taken the position that Arrow discloses a data communication system comprising a VPN management station 160 configured for authentication, encryption, and compression of packets, citing Fig. 13, and Col. 15, lines 52-55 of Arrow.

Applicants respectfully submit that the VPN management station 160 is also a central management station, does not handle packets on the network links, and defines authentication, encryption, and compression parameters for use by other network elements that then handle the

packets. Thus, the VPN management station 160 of Arrow also does not handle packets on the VPN and, accordingly, does not perform at least one of authenticating, encapsulating, and de-encapsulating of the packets that are being metered.

In Arrow, a VPN management station 160 controls VPN units via commands and by passing VPN configuration information to the VPN units. (Arrow at Col. 6, lines 31-34) The configuration information includes applicable encryption, compression, and authentication algorithms. (Arrow at Col. 12, lines 1-10). The configuration information is passed from the VPN management station 160 to the VPN units 115, 125, 135, 145, and 155, to allow them to implement the VPNs defined by the VPN management station 160. (Arrow at Col. 5, lines 51-54; Col. 12, lines 1-10). Thus, the VPN management station defines encryption, compression, and authentication algorithms for use by other network elements – it does not use them itself to handle packets.

Fig. 13, cited by the Examiner, illustrates some of the operations performed by a VPN system manager to create a VPN. (Arrow, Col. 15, lines 29-31). The system manager, is not identified in the figures of Arrow and is mentioned for the first time at Col. 15, line 29 of Arrow. From context, it appears that the system manager is operating through the VPN management station 160 since the actions ascribed to the system manager are taken on the network as a whole. For example, the system manager issues commands to create and define groups of entities that may be nodes on a computer network (state 1304) and defines VPN remote clients that can connect to a VPN from remote locations (state 1306) (See Arrow at Col. 15, lines 40-48). Accordingly, the state 1310 cited by the Examiner, is where the VPN management station 160 defines encryption, compression, and authentication parameters that will then be passed to the VPN units to allow the VPN units to handle traffic on VPN tunnels on the network. These

parameters are not, however, used by the management station 160 to handle packets on the managed links.

Thus, the central control server 160 in Ma does not handle packets of data belonging to an application group, and the VPN management station 160 in Arrow does not handle of packets belonging to an application group. Accordingly, even if Arrow were to be combined with Ma, the resultant server would not handle packets of data belonging to an application group.

Claim 1 states that the VPN server does three things: (1) it assigns a portion of the bandwidth of a remote link to at least one application group, (2) it meters packets belonging to the application group; and (3) it authenticates, encapsulates, or de-encapsulates at least a portion of the packets. The phrase "the packets" in the final "wherein" clause of claim 1 clearly relates back to the packets that are being metered by the VPN server. Thus, claim 1 clearly states that the VPN server must authenticate, encapsulate, or de-encapsulate packets that are metered by the VPN server.

The central control server 160 in Ma may allocate bandwidth on links, but it doesn't actually handle the packets on the link. Thus, it cannot possibly be configured to "at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets." (emphasis added). Similarly, the VPN management station 160 in Arrow does not handle traffic on the VPNs, but rather passes configuration information to the VPN units which handle the traffic. Thus, the VPN management station 160 also cannot be configured to "at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets." A combination of Ma and Arrow therefore would also not handle metered VPN packets, but rather would combine to form a centralized management station configured to interact with ATM switches or VPN units that would then be used to handle the VPN traffic on the network.

During prosecution, applicants explained this difference to the Examiner by focusing on the network architecture. Both Ma and Arrow describe devices (central control server 160 and VPN management station 160 respectively) that operate on the network in a management capacity and interface with network elements via a management interface to cause the network elements to implement the VPNs on the network. The claimed device, by contrast, is a network element that is handling traffic on the VPN.

In the Advisory Action (page 2) the Examiner stated that "Applicant's discussion of the claimed device sits on the end of a VPN tunnel and is configured to manage bandwidth on the tunnel is not considered since the limitations are not recited in the rejected claims." This is incorrect. Claim 1 clearly states that the VPN server is configured to authenticate, encapsulate, or de-encapsulate at least a portion of the metered packets. Since these claimed functions are performed at the end of a VPN tunnel, the Examiner was required to consider these arguments. At the very least, the Examiner was required to show where, within the combination of Ma and Arrow, the asserted combination encapsulated metered packets, de-encapsulated metered packets, or authenticated metered packets. Since the Examiner failed to do so, the rejection must be overturned.

Independent claim 1 recites a method for a VPN server that manages bandwidth of a remote link, comprising assigning a portion of the bandwidth to at least one application group, and metering by the VPN server packets belonging to the application group. Claim 1 further recites that the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets. Thus, the VPN server in independent claim 1 manages bandwidth of a remote link by doing three things: (1) it assigns bandwidth of the remote link to an application group; (2) it meters packets belonging to the application group; and (3) it

authenticates, encapsulates, or de-encapsulates the packets that belong to the application group on the link that is being metered. Since the combination of Ma and Arrow fail to perform this method, the rejection of claim 1 must be reversed.

Independent claims 3, 5, 8, and 9, contain limitations similar to the combination of limitations discussed above. Accordingly, independent claims 3, 5, 8, and 9, and dependent claims 4, 6, and 7, are patentable for at least the same reasons set forth above.

Independent claim 10 recites a system for managing bandwidth of a remote link, comprising: a VPN server, a meter associated with the VPN server for metering packets belonging to the application group, and that the server is a VPN server configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the metered packets. As discussed above, the combination of Ma and Arrow fails to teach or suggest a system of this nature. Accordingly, this claim and similarly drafted independent claims 12, 14, 17, and 18 are patentable over the combination of Ma and Arrow. Dependent claims 13, 15, and 16 are also patentable for at least these same reasons.

Conclusion

Applicants respectfully request that the rejection of claims 1, 3-10, and 12-18 under 35 U.S.C. 103 over Ma and Arrow be reversed.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-13361).

Respectfully Submitted

Dated: June 10, 2004

John C. Gorecki
Registration No. 38,471

John C. Gorecki, Esq.
Patent Attorney
165 Harvard St.
Newton, MA 02460
Tel: (617) 795-0596
Fax: (617) 795-0888

## APPENDIX – PENDING CLAIMS

1. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group; and

metering by the VPN server packets belonging to the application group;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

2. Canceled

3. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group; and

metering by the VPN server packets belonging to the application group;

wherein the VPN server is directly connected to other links having larger bandwidth than the available bandwidth of the remote link; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

4. The method of claim 1 wherein the packets belonging to the application group share a pre-defined configuration.

5. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group; and

metering by the VPN server packets belonging to the application group;

wherein the packets belonging to the application group contend equally for the portion of the bandwidth; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

6. The method of claim 1 wherein metering the packets group further includes metering flow rate of the packets going through the server in either direction.

7. The method of claim 6 wherein metering the packets further includes rejecting the packets if the flow rate exceeds the portion of the assigned bandwidth.

8. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group;

metering by the VPN server packets belonging to the application group; and

allowing a user to specify the bandwidth of the remote link from a user interface;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

9. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group;

metering by the VPN server packets belonging to the application group; and

allowing a user to specify the portion of the assigned bandwidth from a user interface;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

10. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering the packets belonging to the application group;

wherein the server is a VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

11. Canceled

12. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server;

wherein the VPN server is directly connected to other links having larger bandwidth than the available bandwidth of the remote link; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

13. The system of claim 10 wherein the packets belonging to the application group share a pre-defined configuration.

14. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server;

wherein the packets belonging to the application group contend equally for the contention pool; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

15. The system of claim 10 wherein the meter further meters flow rate of the packets going through the server in either direction.

16. The system of claim 15 wherein the meter further rejects the packets if the flow rate exceeds the assigned portion of the bandwidth.

17. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server; and

a user interface that allows a user to specify the bandwidth of the link;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

18. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server; and

a user interface that allows a user to specify the assigned portion of the bandwidth;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.